	Application No.	Applicant(s)
Notice of Allowability	09/707,417	BJORN, VANCE C.
	Examiner	Art Unit
	Aravind K. Moorthy	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *13 September 2007*.

2. ☒ The allowed claim(s) is/are *1-31*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some*   c) ☐ None   of the:

       1. ☐ Certified copies of the priority documents have been received.

       2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

       3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application. **THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

    (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

       1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____ .

    (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of

    Paper No./Mail Date _____ .

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)

3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date <u>see attachment</u>

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application

6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .

7. ☐ Examiner's Amendment/Comment

8. ☒ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____ .

CHRISTOPHER REVAK
PRIMARY EXAMINER

DETAILED ACTION

1. This is in response to the amendment filed on 13 September 2007.

2. Claims 1-31 are pending in the application.

3. Claims 1-31 have been allowed.

Response to Amendment

4. The examiner approves of the amendment made to claims 1, 2, 14, 17, 19, 23, 24 and 27. No new matter has been added to the claims.

5. The amendment made to claims 1, 2, 14, 17, 19, 20, 23, 24 and 27 overcomes the rejection for insufficient antecedent basis.

6. With the amendment made to claims 1 and 17, it is now clear how a record ID being a random number can be authenticated with the user authentication data.

7. With the amendment made to claim 19, it is now clear how the nonce gets to the client.

Allowable Subject Matter

8. Claims 1-31 are allowed.

The following is an examiner's statement of reasons for allowance:

The current application is directed towards a method and apparatus for a third party authentication server is described. The method includes receiving a record ID for a user, and a one-time key generated by the server and encrypted with a user's public key by the server. The method further includes receiving the user's authentication data from the client and determining if the user's authentication data matches the record ID. If the authentication data matches the record ID, decrypting the one-time key with the user's private key, and returning the decrypted one-time key to the client.

The closest prior art to the current application was Hoffman et al U.S. Patent No. 6,594,376 B1 (hereinafter Hoffman). The Hoffman reference provides a method and system for tokenless authorization of commercial transactions between a buyer and a seller using a computer system. The method comprises the steps of registering a buyer, wherein the buyer registers with the computer system a PIN, at least one registration biometric sample, and at least one buyer financial account. The method also includes a seller registration step, wherein the seller registers with the computer system at least one seller financial account. In a proposal step, the seller offers a proposed commercial transaction to the buyer usually comprising price information. If the buyer accepts the seller's proposal, in an acceptance step, the buyer signals his/her acceptance by adding to the proposed commercial transaction the buyer's personal authentication information comprising a PIN and at least one bid biometric sample which is obtained from the buyer's person. In a transmission step, the bid biometric sample and PIN are forwarded to the computer system. The computer system compares the bid biometric sample with registration biometric samples for producing either a successful or failed identification of the buyer in a buyer identification step. Upon determination of sufficient resources, a financial account of the buyer is debited and a financial account of the seller is credited, in a payment step. Therefore, a commercial transaction is conducted without the buyer having to use any portable man-made memory devices such as smartcards or swipe cards.

There are differences between the Hoffman reference and the current application. While the PIN number of Hoffman is pseudo-random, it is not used as, and is not in any way equivalent to a record ID. The PIN number of Hoffman is part of the buyer's personal authentication information, which Hoffman explains comprises a PIN and at least one bid

biometric sample. (Hoffman, Summary, column 4, lines 30-32). The PIN of Hoffman is used

to search for the user in a particular bin of biometrics, thus in Hoffman it is expected that many

users will share the same PIN. (column 9, line 65 to column 10, line 4). It is not used for

identifying a buyer's record. In fact, since Hoffman points out that the PIN is not unique, it

cannot be used to identify a biometric record.

Furthermore, Hoffman teaches away from disassociating biometric data from personally

identifying data, by noting that: Individual Biometric Database (IBD) records store personal

information on buyers for both identification as well as authentication. This information includes

their primary and secondary biometrics, one or more PIN codes, a list of financial accounts,

account index codes, account index names, private code, one or more emergency account index

codes, address, and phone number. The buyer may optionally include this SSN. This

information is necessary for identifying a buyer either by biometric or personal information, for

accessing related information, or for providing an address or phone number to remote sellers for

additional verification (Hoffman, column 33, lines 16-21). Thus, it is clear that in Hoffman, the

biometric record is associated not only with a name, but also with an address, and social security

number. This is clearly not an anonymous record, in which the biometric is not associated with

identifying information. Thus, if a database is compromised, the hacker in Hoffman will

certainly know the user's name, address, and biometric. In contrast, claim 1 recites in part

"receiving a record ID for a user, the record ID being a random number generated for tracking

authentication data and disassociating the authentication data from other client identity data."

As noted above, Hoffman specifically teaches away from a record ID being a random number

used for tracking authentication data and for disassociating the authentication data from

other client identity data. The PIN of Hoffman is linked to the biometric and name/address data. This is further illustrated in Figure 10, which shows the elements of the biometric record, including the biometric data, name, account data, etc. The name and account data is client identity data, which is stored as part of the biometric record in Hoffman. Therefore, Hoffman does not teach or suggest disassociating the authentication data from other client identity data. Therefore, claim 1, and claims 2-13 which depend on it, are not obvious over Hoffman. Claim 14 recites in part "looking up a record ID associated with the user, the record ID being a random number generated to track the user's authentication data and used to separate the user's other identity information from the authentication data." As noted above, Hoffman specifically teaches away from a record ID used to separate the user's other identity information from the authentication data. Therefore, claim 14, and claims 15-16 which depend on it, are not obvious over Hoffman. Claim 17 similarly recites in part: "the record ID being a randomly generated number used to separate the user's other identity information from the user's authentication data." As noted above, Hoffman specifically teaches away from a record ID randomly generated to separate the user's identity from authentication data. Therefore, claim 17, and claims 18-31 which depend on it, are not obvious over Hoffman.

Any claims not directly addressed are allowed on the virtue of their dependency

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

9.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy
November 20, 2007

CHRISTOPHER REVAK
PRIMARY EXAMINER